Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 26 juin 2013
N° CERTA-2013-AVI-374

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTA-2013-AVI-374
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	26 juin 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla du MFSA2013-49 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-50 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-51 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-52 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-53 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-54 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-55 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-56 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-57 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-58 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-59 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-60 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-61 25 juin 2013 Bulletin de sécurité Mozilla du MFSA2013-62 25 juin 2013
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque(s)

- exécution de code arbitraire à distance
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données

2 Systèmes affectés

- Mozilla Firefox versions antérieures à 22.0
- Mozilla Firefox ESR versions antérieures à 17.0.7
- Mozilla Thunderbird versions antérieures à 17.0.7
- Mozilla Thunderbird ESR versions antérieures à 17.0.7

3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits *Mozilla*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Mozilla du MFSA2013-49 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-49.html
- Bulletin de sécurité Mozilla du MFSA2013-50 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-50.html
- Bulletin de sécurité Mozilla du MFSA2013-51 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-51.html
- Bulletin de sécurité Mozilla du MFSA2013-52 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-52.html
- Bulletin de sécurité Mozilla du MFSA2013-53 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-53.html
- Bulletin de sécurité Mozilla du MFSA2013-54 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-54.html
- Bulletin de sécurité Mozilla du MFSA2013-55 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-55.html
- Bulletin de sécurité Mozilla du MFSA2013-56 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-56.html
- Bulletin de sécurité Mozilla du MFSA2013-57 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-57.html
- Bulletin de sécurité Mozilla du MFSA2013-58 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-58.html
- Bulletin de sécurité Mozilla du MFSA2013-59 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-59.html
- Bulletin de sécurité Mozilla du MFSA2013-60 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-60.html
- Bulletin de sécurité Mozilla du MFSA2013-61 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-61.html
- Bulletin de sécurité Mozilla du MFSA2013-62 25 juin 2013
  http://www.mozilla.org//security/announce/2013/mfsa2013-62.html
- Référence CVE CVE-2013-1682
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1682
- Référence CVE CVE-2013-1683
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1683
- Référence CVE CVE-2013-1684
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1684

- Référence CVE CVE-2013-1685
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1685
- Référence CVE CVE-2013-1686
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1686
- Référence CVE CVE-2013-1687
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1687
- Référence CVE CVE-2013-1688
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1688
- Référence CVE CVE-2013-1690
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1690
- Référence CVE CVE-2013-1692
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1692
- Référence CVE CVE-2013-1693
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1693
- Référence CVE CVE-2013-1694
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1694
- Référence CVE CVE-2013-1695
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1695
- Référence CVE CVE-2013-1696
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1696
- Référence CVE CVE-2013-1697
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1697
- Référence CVE CVE-2013-1698
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1698
- Référence CVE CVE-2013-1699
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1699
- Référence CVE CVE-2013-1700
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1700

Gestion détaillée du document

26 juin 2013 version initiale.